LISTING OF THE CLAIMS

Claim 25. (Canceled)

26. (Currently Amended) The method according to claim [[25]] 40, wherein the carrier signal includes a stream of digital samples.

27. (Currently Amended) The method according to claim [[25]] 40, wherein the carrier signal includes a continuous analog waveform.

28. (Currently Amended) The method according to claim [[25]] 40, wherein the digital watermark, includes at least one selected from the group consisting of: rights ownership identification, authorship identification of the encoded carrier signal, ownership identification of a unique copy of the encoded carrier signal, and a serialization code uniquely identifying a copy of the encoded carrier signal.

29. (Canceled).

30. (Currently Amended) The method according to claim [[29]] 46, wherein the carrier signal includes a stream of digital samples.

31. (Currently Amended) The method according to claim [[29]] 46, wherein the carrier signal includes a continuous analog waveform.

32. (Currently Amended) The method according to claim [[29]] 46, wherein the digital watermark includes at least one selected from the group consisting of: rights ownership identification, authorship identification of the encoded carrier signal, ownership identification of a unique copy of the encoded carrier signal, and a serialization code uniquely identifying a copy of the encoded carrier signal.

33. (Canceled)

34. (Currently Amended) ~~The method according to claim 33, further~~ A method for steganographically protecting a digital signal comprising the step of:

a) providing a carrier signal;

b) using a stega-cipher to steganographically encode independent information including a digital watermark into the carrier signal;

c) generating a first derivative encoded signal representing the original carrier signal combined with the encoded independent information, including the digital watermark, wherein the first derivative encoded signal is an arbitrarily close approximation of the original carrier signal; and

d) modifying the first derivative encoded signal to produce a second derivative encoded signal, wherein the second derivative encoded signal differs from the original carrier signal by a greater degree than the first derivative encoded signal differs from the original carrier signal, as measured by an arbitrary signal metric.

35. (Canceled).

36. (Currently Amended) The method according to claim [[29]] 46, further comprising the step of:

~~e)~~ ——decoding a single message bit from a single sample by reading a ~~simple~~ single bit of the single sample as the message bit.

37. (Currently Amended) The method according to claim [[29]] 46, further comprising the step of:

~~e)~~ ——decoding a ~~signal~~ single message bit from a single sample by mapping the single sample in the range of sample values which indicate a particular message bit value.

38. (Currently Amended) The method according to claim [[29]] 46, further comprising the step of:

~~e)~~ ——decoding a single message bit from a ~~signal~~ single spectral value by mapping the single spectral value into a range of sample values which indicate a particular message bit value.

39. (Currently Amended) The method according to claim [[25]] 40, further comprising the step of:

~~e)~~ ——using a map table to define where watermark information is to be encoded into the carrier signal based on the random or pseudo-random masks ~~into the carrier signal~~, wherein the map table is defined such that any index of the map table enables encoding of information.

40. (Currently Amended) ~~The method according to claim 25, further~~ A method for steganographically protecting a digital signal comprising the step of:

a) providing a carrier signal;

b) using a stega-cipher to steganographically encode independent information including a digital watermark into the carrier signal;

c) selecting a mask set, said mask ~~stet~~ set including one or more random or pseudo-random series of bits, referred to as masks;

d) selecting a random or pseudo-random start of message delimiter; and

e) selecting independent information to be encoded.

41. (Previously Presented) The method according to claim 40, further comprising the step of:

f) generating a message bit stream to be encoded such that the stream includes:

1) the random or pseudo-random start of message delimiter;

2) a number of message bytes to follow the message; and

3) the independent information.

42. (Previously Presented) The method according to claim 41, further comprising the step of:

g) separating an input sample stream into smaller discrete sample windows comprising segments of the input sample stream.

43. (Currently Amended) The method according to claim 42, further comprising of the step of:

h) using positions within the sample windows and a position within the input stream to index random or pseudo-random masks and compute a mapping function to determine encoding positions and encode digital watermark information into the sample windows.

44. (Currently Amended) The method according to claim 43, further comprising the step of:

i) computing a spectral transform of the sample windows prior to digital watermark data encoding.

45. (Previously Presented) The method according to claim 44, further comprising the step of:

j) computing an inverse spectral transform of the encoded spectral transform data after digital watermark data encoding.

46. (Currently Amended) ~~The method according to claim 29, further~~ A method for steganographically protecting a digital signal comprising the steps of:

a) providing a carrier signal that has been encoded with independent information;

b) using a stega-cipher to steganographically decode independent information including a digital watermark from the carrier signal;

c) selecting a mask set, said mask set including one or more random or pseudo-random series of bits, referred to as masks;

d) selecting a random or pseudo-random start of message delimiter; and

e) selecting an input sample stream to be decoded.

47. (Previously Presented) The method according to claim 46, further comprising the step of:

f) separating the input sample stream into smaller discrete sample windows comprising segments of the input sample stream.

48. (Previously Presented) The method according to claim 47, further comprising the step of:

g) using positions within one of the sample windows and a position within the input stream to index random or pseudo-random masks and compute a mapping function to determine decoding positions and to decode digital watermark information from the sample window.

49. (Previously Presented) The method according to claim 48, further comprising the step of:

h) computing a spectral transform of the sample window prior to digital watermark data decoding.

50. (Previously Presented) The method according to claim 41, wherein the independent information contains, at least one selected from the group consisting of: a hash value computed on the start of message delimiter, and a digital signature of the start of message delimiter.

51. (Previously Presented) The method according to claim 48, further comprising the step of:

h) validating at least one selected from the group consisting of:

(1) a hash value computed on the start of message delimiter, and

(2) a digital signature of the start of message delimiter,

wherein the step h) of validating occurs after the start of message delimiter and the encoded information of said hash value or said digital signature have been decoded and the validation consists of computing an appropriate result using the start of message delimiter, comparing it to a value in the decoded data, and verifying any signature.

52. (Currently Amended) The method according to claim [[25]] 40, further comprising the step of:

~~e)~~ adding unique data to each individual watermark, rendering it distinct from any other watermark in the same sample stream.

53. (Currently Amended) The method according to claim 52, further comprising the step of:

~~d)~~ pre-processing sample windows in the sample stream to be watermarked.

54. (Currently Amended) The method according to claim 53, further comprising the step of:

~~e)~~ determining which sample windows will contain the individual digital watermark to be encoded.

55. (Currently Amended) The method according to claim 54, further comprising the step of:

~~f)~~——calculating a size of the independent information comprising the digital watermark plus a size of an added hash value to determine a number of sample windows required to contain a complete watermark.

56. (Currently Amended) The method according to claim 55, further comprising the step of:

~~g)~~——computing a secure one way hash function of the carrier signal data in said sample windows, wherein said hash function is insensitive to changes introduced into the carrier signal for the purpose of carrying digital watermark information.

57. (Currently Amended) The method according to claim 56, further comprising the step of:

~~h)~~——concatenating the hash value with the independent information, creating an expanded, unique digital watermark.

58. (Currently Amended) The method according to claim [[29]] 46, further comprising the step of:

~~e)~~——obtaining a unique hash value contained in the independent information comprising part of the digital watermark.

59. (Currently Amended) The method according to claim 58, further comprising the additional step of:

~~d)~~——re-processing sample windows in the sample stream which contained the decoded watermark.

60. (Currently Amended) The method according to claim 59, further comprising the step of:

~~e)~~ computing a secure one way hash function of the carrier signal data in said sample windows, wherein said hash function is insensitive to changes introduced into the carrier signal for the purpose of carrying digital watermark information.

61. (Currently Amended) The method according to claim 60, further comprising the step of:

~~f)~~ comparing the computed hash value to the value contained in the watermark.

62. (Currently Amended). The method ~~of~~ according to claim [[25]] 40, wherein the step of steganographically encoding independent information into the carrier signal causes an imperceptible change in the carrier signal.

63. (Currently Amended) The method ~~of~~ according to claim [[29]] 46, wherein the step of steganographically decoding independent information into the carrier signal causes an imperceptible change in the carrier signal.